

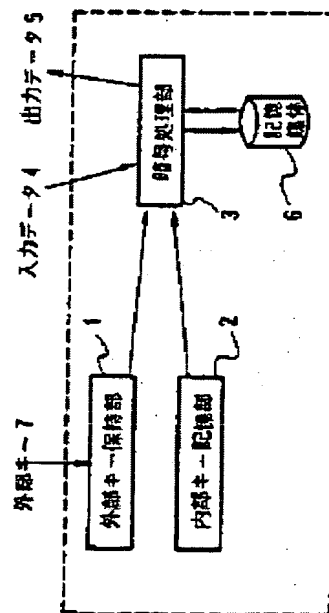
• INFORMATION MEMORY

Patent number: JP63182758
Publication date: 1988-07-28
Inventor: NAKAKUKI YOICHIRO
Applicant: NIPPON ELECTRIC CO
Classification:
- International: G06F9/06; G06F12/14; G09C1/00; G06F9/06;
G06F12/14; G09C1/00; (IPC1-7): G06F9/06;
G06F12/14; G09C1/00
- european:
Application number: JP19870014903 19870123
Priority number(s): JP19870014903 19870123

Report a data error here

Abstract of JP63182758

PURPOSE: To secure the high safety by combining the external input keys with the internal keys proper to each device for ciphering. CONSTITUTION: An external key holding part 1 stores the external input keys and an internal key memory part 2 stores the internal keys proper to each device. The data supplied from outside are ciphered via the external and internal keys and stored in a memory means 6. Thus it is possible to make it extremely hard to read correctly the recorded contents with only the keys set from outside. While the recorded contents can be easily copied to another medium and only the device used for writing can read out correctly the decoded information. As a result, it is impossible to use the recorded programs, etc., although they can be copied.



Data supplied from the esp@cenet database - Worldwide

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

昭63-182758

⑬ Int. Cl.

識別記号

庁内整理番号

⑭ 公開 昭和63年(1988)7月28日

G 06 F 12/14

3 2 0

B-7737-5B

G 09 C 9/06

3 3 0

A-7361-5B

G 09 C 1/00

7368-5B

審査請求 未請求 発明の数 1 (全4頁)

⑮ 発明の名称 情報記憶装置

⑯ 特 願 昭62-14903

⑰ 出 願 昭62(1987)1月23日

⑱ 発 明 者 中 莖 洋 一 郎 東京都港区芝5丁目33番1号 日本電気株式会社内

⑲ 出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号

⑳ 代 理 人 弁理士 内 原 晋

明 細 書

発 明 の 名 称 情報記憶装置

特 許 請 求 の 範 囲

外部より入力されるキーを格納する手段と、装置固有の内部キーを記憶する手段と、情報を記憶する記憶手段と、外部より入力されるデータを前記外部キー及び内部キーを用いて暗号化して前記記憶手段に格納すると共に、前記記憶手段より読み出された情報を前記外部、内部キーを用いて復号する暗号処理部とから構成される情報記憶装置。

発 明 の 詳 細 な 説 明

(産業上の利用分野)

本発明は暗号化方式を用いた情報記憶装置である。

(従来の技術)

記憶媒体上のデータの守秘、記憶されたプログラム等の複製使用の防止の方法として、次のよう

な方法が知られている。データの守秘に関しては、元のデータを暗号化してから媒体上に格納する方法が知られており、これは暗号化のためのキーを用いて暗号化及び復号を行う方法である。また一方、プログラム等を複写して複数の装置上で使用されることを防止するための方法として知られているのは、媒体に特殊なフォーマットを施したり、セクタ長を変える等の特別な記録の方式を採用する方法である。

(発明が解決しようとする問題点)

まず、暗号化によるデータ守秘法においては、暗証番号等のキーの値さえ分かれば暗号文を平文に復号することができるという危険性を持っている。本発明の第一の目的はこのようなキーの盗難等に対する安全性を高めることである。

また、記憶媒体にプログラム等を特殊な形式で記録して複写を防止した場合、それを読み出すためのプログラム等を解析することにより記録の形式が解明されてしまう恐れがある。また、この場合バックアップ用の媒体を作成することも妨げて

のメモリ部に書き込む方法をとるもので、LSIの機能として、その内部キーの書き込み機能を持たせ、読み取り機能を持たせないことにより外部からの内部キー値の読みだしを防ぐことができる。あるいは一般のPROM等を利用して内部キーを格納する場合には、LSIの端子・配線等を完全に絶縁する等の方法で、外部からの読みだしを不可能にすることが可能である。

(発明の効果)

従来、外部から入力されるキーの値のみによって暗号化を行っていたのに対して、本発明では各装置に固有の内部キーと組み合わせて実際の暗号化を行うため、万一外部キーの値を知ることが出来ても実際に暗号化された文を正しく読み出すためには、事実上計算不可能であるような膨大な計算量を必要とさせることが可能であるため、より高い安全性を確保することが可能となった。

また、媒体に記録されたデータの複写は許すかわりに装置内部に保持されたキーの複製を防ぐことにより、データやプログラムのバックアップを

可能としつつも複製使用を防止することが可能となった。

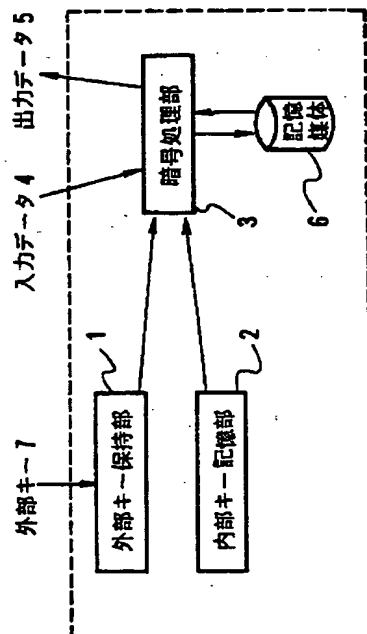
図面の簡単な説明

第1図は本装置の基本的な構成を示す図で、第2図は情報守秘に応用した場合の構成図、第3図は外部記憶媒体を対象とした場合の構成図、第4図は外部記憶媒体上のプログラムの複製使用防止に応用した場合の構成図である。

図において、1は外部キー保持部、2は内部キー記憶部、3は暗号処理部、4は入力データ、5は出力データ、6は記憶媒体、7は外部キー、8は取り外し可能とした内部キー記憶部、9は取り外しが可能な記憶媒体。

代理人 弁理士 内原 晋

第 1 図



第 2 図

